

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-157837

(43)Date of publication of application : 29.05.1992

(51)Int.Cl.

H04L 9/28

H04K 1/02

(21)Application number : 02-283195

(71)Applicant : FUJITSU LTD

(22)Date of filing : 20.10.1990

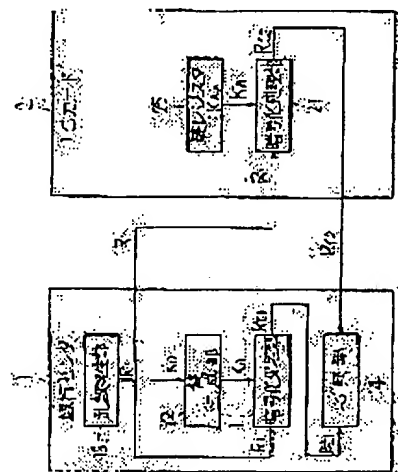
(72)Inventor : HASEBE TAKAYUKI
AKIYAMA RYOTA

(54) KEY SUPPLY SYSTEM FOR CIPHER PROCESSING

(57)Abstract:

PURPOSE: To apply cipher processing based upon a DES system even to a device whose storage means quantity is limited by providing a an IC card with a key register as a key storage means.

CONSTITUTION: A bank center 1 is provided with a encipherment processing part 11, a key generation part 12, a random number generation part 13, and a comparison part 14, but the IC card 2 is provided with the key register 25 instead of the key generation part 23. The random number generation part 13 provided in the bank center 1 generates and inputs a random number R1 to the encipherment processing part 11, and also transfers the random number even to the IC card 2, so that it is inputted to its encipherment part 21. The encipherment processing parts 11 and 21 convert the input random number R1 into enciphered random numbers RC1 and RC2, which are sent to the comparison part 14 provided in the bank center 1 and compared with each other, so that the bank center 1 authenticates the IC card 2 when both the random number are equal to each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平4-157837

⑬ Int. Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成4年(1992)5月29日

H 04 L 9/28
H 04 K 1/02

7117-5K
7117-5K

H 04 L 9/02

A

審査請求 未請求 請求項の数 6 (全15頁)

⑮ 発明の名称 暗号処理用鍵供給方式

⑯ 特 願 平2-283195

⑰ 出 願 平2(1990)10月20日

⑱ 発 明 者 長 谷 部 高 行 神奈川県川崎市中原区上小田中1015番地 富士通株式会社
内

⑲ 発 明 者 秋 山 良 太 神奈川県川崎市中原区上小田中1015番地 富士通株式会社
内

⑳ 出 願 人 富士通株式会社 神奈川県川崎市中原区上小田中1015番地

㉑ 代 理 人 弁理士 井 桁 貞一

明 細 書

1. 発明の名称

暗号処理用鍵供給方式

2. 特許請求の範囲

【1】平文(P)と暗号文(C)との間の変換処理をDES方式に基づき実行する暗号化処理部(21)を具備し、相手装置(200)との間で暗号通信を実行する装置(100)において、

前記装置(100)外で生成された、前記暗号化処理部(21)が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵(K_a)および復号鍵(K_d)の少なくとも何れかを記憶し、前記暗号化処理部(21)に供給する鍵記憶手段(101)を設けることを特徴とする暗号処理用鍵供給方式。

【2】平文(P)と暗号文(C)との間の変換処理をDES方式に基づき実行する暗号化処理部(21)を具備し、相手装置(200)との間で暗号通信を実行する装置(100)において、

前記装置(100)外で生成された、前記暗号化処理部(21)が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵(K_a)を記憶する暗号鍵記憶手段(102)と、

前記暗号鍵記憶手段(102)が記憶する前記暗号鍵(K_a)を抽出し、各十六段の順序を反転させて復号鍵(K_d)を生成し、前記暗号化処理部(21)に供給する反転処理手段(103)とを設けることを特徴とする暗号処理用鍵供給方式。

【3】平文(P)と暗号文(C)との間の変換処理をDES方式に基づき実行する暗号化処理部(21)を具備し、相手装置(200)との間で暗号通信を実行する装置(100)において、

前記装置(100)外で生成された、前記暗号化処理部(21)が前記変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分のマスク鍵(K_m)を記憶するマスク鍵記憶手段(105)と、

前記相手装置(200)と共用する48×16

ビットから成る同一の乱数を、共有するマスタ鍵 (K_m) を用いてDES方式に基づき暗号化処理し、それぞれ48ビットから成る十六段分のセッション暗号鍵 (K_{ss}) を生成する暗号処理手段 (104) と、

前記暗号処理手段 (104) が生成する前記セッション暗号鍵 (K_{ss}) の、各十六段の順序を反転させてセッション復号鍵 (K_{ss}) を生成し、前記暗号化処理部 (21) に供給する反転処理手段 (103) とを設けることを特徴とする暗号処理用鍵供給方式。

【4】入力情報を暗号化処理部 (21) によりDES方式に基づき暗号化処理し、暗号処理結果を相手装置 (400) との間で比較することにより相手装置 (400) を認証する装置 (300) において、

前記装置 (300) 外で生成された、前記暗号化処理部 (21) が前記暗号処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の認証鍵 (K_a) を記憶し、前記暗号化処理部

(21) に供給する認証鍵記憶手段 (301) を設けることを特徴とする暗号処理用鍵供給方式。

【5】前記暗号鍵 (K_s)、復号鍵 (K_d)、マスタ鍵 (K_m) および認証鍵 (K_a) は、パリティビットを含む64ビットから成るオリジナル鍵から、DES方式に基づき生成されることを特徴とする請求項1、2、3または4記載の暗号処理用鍵供給方式。

【6】前記暗号鍵 (K_s)、復号鍵 (K_d)、マスタ鍵 (K_m) および認証鍵 (K_a) は、パリティビットを含む64ビットから成るオリジナル鍵から、前記DES方式に基づくことなく生成されることを特徴とする請求項1、2、3または4記載の暗号処理用鍵供給方式。

3. 発明の詳細な説明

(概要)

DES方式に基づく暗号処理を採用する暗号通信システム、或いは認証システムにおける暗号処理用鍵供給方式に関し、

3

収容すべき手段を極力減少させることにより、収容手段量に制限のある装置においてもDES方式に基づく暗号処理を適用可能とすることを目的とし、

平文と暗号文との間の変換処理をDES方式に基づき実行する暗号化処理部を具備し、相手装置との間で暗号通信を実行する装置において、装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵および復号鍵の少なくとも何れかを記憶し、暗号化処理部に供給する鍵記憶手段を設ける様に構成し、また装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の暗号鍵を記憶する鍵記憶手段と、鍵記憶手段が記憶する暗号鍵を抽出し、各十六段の順序を反転させて復号鍵を生成し、暗号化処理部に供給する反転処理手段とを設ける様に構成し、また装置外で生成された、暗号化処理部が変換処理を実行する為に必要とするそれぞれ48ビットから成る十六段分のマ

4

スタ鍵を記憶するマスタ鍵記憶手段と、相手装置と共用する48×16ビットから成る同一の乱数を、共有するマスタ鍵を用いてDES方式に基づき暗号化処理し、それぞれ48ビットから成る十六段分のセッション暗号鍵を生成する暗号処理手段と、暗号処理手段が生成するセッション暗号鍵の、各十六段の順序を反転させてセッション復号鍵を生成し、暗号化処理部に供給する反転処理手段とを設ける様に構成し、また入力情報を暗号化処理部によりDES方式に基づき暗号化処理し、暗号処理結果を相手装置との間で比較することにより相手装置を認証する装置において、装置外で生成された、暗号化処理部が暗号処理を実行する為に必要とするそれぞれ48ビットから成る十六段分の認証鍵を記憶し、暗号化処理部に供給する認証鍵記憶手段を設ける様に構成し、なお暗号鍵、復号鍵、マスタ鍵および認証鍵は、パリティビットを含む64ビットから成るオリジナル鍵から、DES方式に基づき生成される様に構成し、またDES方式に基づくことなく生成される様に構成

5

6

する。

(産業上の利用分野)

本発明は、DES方式に基づき暗号処理を採用する暗号通信システム、或いは認証システムにおける暗号処理用鍵供給方式に関する。

所要の情報を、第三者に秘匿して所定の相手との間で授受する暗号処理の一つとして、米国商務省により制定公布されたデータ暗号化規格(Data Encryption Standard、以後DESと称する)が公知である。

一方、例えば銀行における窓口の無人化に伴い、顧客が所持するICカードと銀行センタとの間で、第三者に秘匿すべき情報の授受、或いは情報授受相手の認証に、前述のDES方式を採用する機会が増加しつつある。

(従来技術)

第10図は従来ある暗号通信システムの一例を示す図であり、第11図は第10図における銀行センタ

側装置の一例を示す図であり、第12図は第10図におけるICカード側装置の一例を示す図である。

第10図において、銀行センタ1には、入力される明文PをDES方式に基づき暗号文Cに変換する暗号化処理部11と、銀行センタ1およびICカード2が第三者に秘匿して保有する、パリティビットを含む64ビットから成るオリジナル鍵K。から、暗号化処理部11が暗号化を実行する為に必要とする、それぞれ48ビットから成る十六段分の暗号鍵K。を生成する鍵生成部12とが設けられ、またICカード2には、銀行センタ1から転送される暗号文Cを、DES方式に基づき明文Pに変換する暗号化処理部21と、銀行センタ1およびICカード2が第三者に秘匿して保有する、パリティビットを含む64ビットから成るオリジナル鍵K。から、暗号化処理部21が復号化を実行する為に必要とする、それぞれ48ビットから成る十六段分の復号鍵K。を生成する鍵生成部22とが設けられている。

第11図において、鍵生成部12は、公知の如く、

オリジナル鍵K。を蓄積するレジスタREG、第一縮約型転置部PC-1、十六段分の左シフトS F-L、第二縮約型転置部PC-2および各種レジスタREG類から構成され、オリジナル鍵K。から十六段分の暗号鍵K。 (各段の暗号鍵をそれぞれ第一段暗号鍵K₀₁乃至第十六段暗号鍵K₀₁₆と称する)を生成し、暗号化処理部11の各段に供給する。

また暗号化処理部11は、公知の如く、入力される明文Pを64ビット宛蓄積するレジスタREG、初期転置部IP、十六段分の暗号関数部f、排他論理和部(+)、レジスタREG類、最終転置部IP⁻¹、出力される暗号文Cを64ビット宛蓄積するレジスタREGから構成され、鍵生成部12から各段の暗号関数部fにそれぞれ暗号鍵K₀₁乃至K₀₁₆を供給することにより、入力される明文Pを64ビット宛、暗号文Cに変換して出力する。

一方第12図において、鍵生成部22は、公知の如く、鍵生成部12(第11図)における各左シフ

タS F-Lを右シフトS F-Rに変更することにより、オリジナル鍵K。から十六段分の復号鍵K。 (各段の復号鍵をそれぞれ第一段復号鍵K₀₁乃至第十六段復号鍵K₀₁₆と称する)を生成し、暗号化処理部21の各段に供給する。

また暗号化処理部21は、公知の如く、入力される暗号文Cを64ビット宛蓄積するレジスタREG、初期転置部IP、十六段分の暗号関数部f、排他論理和部(+)、レジスタREG類、最終転置部IP⁻¹、出力される明文Pを64ビット宛蓄積するレジスタREGから構成され、鍵生成部22から各段の暗号関数部fにそれぞれ復号鍵K₀₁乃至K₀₁₆を供給することにより、入力される暗号文Cを、明文Pに変換して出力する。

なおDES方式においては、鍵生成部12が暗号化処理部11の各段に供給する第一段暗号鍵K₀₁乃至第十六段暗号鍵K₀₁₆と、鍵生成部22が暗号化処理部21の各段に供給する第一段復号鍵K₀₁乃至第十六段復号鍵K₀₁₆とを、K₀₁=K₀₁₆、K₀₂=K₀₁₅、……、K₀₁₆=K₀₁となる如

く生成することにより、暗号化処理部 11 と 21 とを同一構成としている。

次に第13図は従来ある認証システムの一例を示す図である。

第13図において、銀行センタ 1 には前述の暗号化処理部 11 および鍵生成部 12 の他に、乱数 R を発生する乱数発生部 13 と、比較部 14 とが設けられており、また IC カード 2 には、前述と暗号化処理部 21 と、銀行センタ 1 に設けられている鍵生成部 12 と同一構成を有する鍵生成部 23 とが設けられている。

銀行センタ 1 に設けられている鍵生成部 12 と、IC カード 2 に設けられている鍵生成部 23 とは、それぞれ保有されている同一のオリジナル鍵 K から、それぞれ 48 ビットから成る十六段分の認証鍵 K を生成し、それぞれ暗号化処理部 11 および 21 の各段に供給する。

一方銀行センタ 1 に設けられている乱数発生部 13 は、乱数 R を発生して暗号化処理部 11 に入力すると共に、IC カード 2 にも転送し、暗号

化処理部 21 に入力する。

各暗号化処理部 11 および 21 は、それぞれ鍵生成部 12 および 23 から認証鍵 K を供給することにより、入力される乱数 R を、それぞれ暗号化乱数 R_{e1} および R_{e2} に変換し、銀行センタ 1 に設けられた比較部 14 に伝達する。

比較部 14 は、暗号化処理部 11 から伝達される暗号化乱数 R_{e1} と、暗号化処理部 21 から伝達される暗号化乱数 R_{e2} とを比較し、両者が一致した場合には、銀行センタ 1 は IC カード 2 を認証する。

〔発明が解決しようとする課題〕

以上の説明から明らかな如く、従来ある暗号通信システムにおいては、IC カード 2 に鍵生成部 22 を設ける必要があり、また従来ある認証システムにおいても、IC カード 2 に鍵生成部 23 を設ける必要があり、IC カード 2 に収容し切れぬ問題があった。

本発明は、収容すべき手段を極力減少させるこ

1 1

とにより、収容手段量に制限のある装置においても DES 方式に基づく暗号処理を適用可能とすることを目的とする。

〔課題を解決するための手段〕

第 1 図は本発明の原理を示す図であり、同図 (a) は請求項 1 に関する原理を示し、同図 (b) は請求項 2 に関する原理を示し、同図 (c) は請求項 3 に関する原理を示し、同図 (d) は請求項 4 に関する原理を示す。

第 1 図において、100 は暗号通信を行う装置、200 は装置 100 との間の暗号通信の相手装置、300 は認証を行う装置、400 は装置 300 との認証の相手装置、11 は相手装置 200 が具備する暗号化処理部、21 は装置 100 および 300 が具備する暗号化処理部である。

101 は、本発明（請求項 1）により装置 100 に設けられた鍵記憶手段である。

102 は、本発明（請求項 2）により装置 100 に設けられた暗号鍵記憶手段である。

1 2

103 は、本発明（請求項 2 および請求項 3）により装置 100 に設けられた反転処理手段である。

104 は、本発明（請求項 3）により装置 100 に設けられた暗号処理手段である。

105 は、本発明（請求項 3）により装置 100 に設けられたマスク鍵記憶手段である。

301 は、本発明（請求項 4）により装置 300 に設けられた認証鍵記憶手段 301 である。

〔作用〕

暗号化処理部 21 は、平文 P と暗号文 C との間の変換処理を DES 方式に基づき実行する。

鍵記憶手段 101 は、装置 100 外で生成された、暗号化処理部 21 が変換処理を実行する為に必要とする、それぞれ 48 ビットから成る十六段分の暗号鍵 K および復号鍵 K の少なくとも何れかを記憶し、暗号化処理部 21 に供給する。

暗号鍵記憶手段 102 は、装置 100 外で生成された、暗号化処理部 21 が変換処理を実行する

1 3

1 4

為に必要とする、それぞれ48ビットから成る十六段分の暗号鍵 K_0 を記憶する。

反転処理手段103は、暗号鍵記憶手段102が記憶する暗号鍵 K_0 を抽出し、各十六段の順序を反転させて復号鍵 K_1 を生成し、暗号化処理部21に供給する。

マスタ鍵記憶手段105は、装置100外で生成された、暗号化処理部21が変換処理を実行する為に必要とする、それぞれ48ビットから成る十六段分のマスタ鍵 K_m を記憶する。

暗号処理手段104は、相手装置200と共用する 48×16 ビットから成る同一の乱数を、共有するマスタ鍵 K_m を用いてDES方式に基づき暗号化処理し、それぞれ48ビットから成る十六段分のセッション暗号鍵 K_s を生成する。

認証鍵記憶手段301は、装置300外で生成された、暗号化処理部21が暗号処理を実行する為に必要とする、それぞれ48ビットから成る十六段分の認証鍵 K_a を記憶し、暗号化処理部21に供給する。

なお暗号鍵 K_0 、復号鍵 K_1 、マスタ鍵 K_m および認証鍵 K_a は、パリティビットを含む64ビットから成るオリジナル鍵から、DES方式に基づき生成されることが考慮される。

また暗号鍵 K_0 、復号鍵 K_1 、マスタ鍵 K_m および認証鍵 K_a は、パリティビットを含む64ビットから成るオリジナル鍵から、DES方式に基づくことなく生成されることが考慮される。

従って、本発明(請求項1乃至請求項6)によれば、装置にはDES方式に基づく暗号処理に必要な鍵生成部を設ける必要がなくなり、装置の小形化、軽量化および経済化を大幅に向上する。

【実施例】

以下、本発明の一実施例を図面により説明する。第2図は本発明(請求項1および請求項5)の一実施例による暗号通信システムを示す図であり、第3図は本発明(請求項2および請求項5)の一実施例による暗号通信システムを示す図であり、第4図は第3図における反転処理部の一例を示す

15

図であり、第5図は第3図に対応する双方向暗号通信システムを示す図であり、第6図は本発明(請求項2および請求項6)の一実施例による暗号通信システムを示す図であり、第7図は本発明(請求項3および請求項5)の一実施例による暗号通信システムを示す図であり、第8図は本発明(請求項4および請求項5)の一実施例による認証システムを示す図であり、第9図は本発明(請求項4および請求項6)の一実施例による認証システムを示す図である。なお、全図を通じて同一符号は同一対象物を示す。また装置100は何れもICカードとし、相手装置200は何れも銀行センタ1とする。

第2図においては、第1図(a)における鍵記憶手段101として鍵レジスタ24が設けられ、また第3図においては、第1図(b)における暗号鍵記憶手段102として鍵レジスタ25が設けられ、また第1図(b)における反転処理手段103として反転処理部26が設けられ、また第6図においては、第1図(b)における暗号鍵記憶

16

手段102として鍵レジスタ27が設けられ、また第1図(b)における反転処理手段103として反転処理部26が設けられ、また第7図においては、第1図(c)における暗号鍵記憶手段102として鍵レジスタ44が設けられ、また第1図(c)における暗号処理手段104として暗号化処理部21が使用され、また第1図(c)における反転処理手段103として反転処理部45が設けられ、また第8図においては、第1図(d)における認証鍵記憶手段301として鍵レジスタ25が設けられ、また第9図においては、第1図(d)における認証鍵記憶手段301として鍵レジスタ27が設けられている。

最初に、第2図乃至第7図に基づき本発明の一実施例による暗号通信システムを説明する。

第2図において、銀行センタ1には、前述(第10図)と同様の暗号化処理部11および鍵生成部12が設けられており、鍵生成部12は、パリティビットを含む64ビットから成るオリジナル鍵 K_0 から、それぞれ48ビットから成る十六段分

17

18

の暗号鍵 K_1 、および復号鍵 K_1 を生成する。

一方ICカード2には、第10図における鍵生成部22の代わりに鍵レジスタ24が設けられ、銀行センタ1において鍵生成部12が生成する復号鍵 K_1 が蓄積されている。

銀行センタ1においては、前述(第10図)と同様の過程で、暗号化処理部11が鍵生成部12から暗号鍵 K_1 を供給されることにより、入力される平文Pを暗号文Cに変換し、ICカード2に転送する。

ICカード2における暗号化処理部21は、鍵レジスタ24に蓄積済の復号鍵 K_1 を供給されることにより、前述(第10図)と同様の過程で、銀行センタ1から転送される暗号文Cを平文Pに変換し、出力する。

次に第3図において、銀行センタ1には、前述(第10図)と同様に暗号化処理部11および鍵生成部12が設けられており、鍵生成部12は、前述(第10図)と同様に、オリジナル鍵 K_1 から暗号鍵 K_1 を生成して暗号化処理部11に供給し、

暗号化処理部11は、前述(第2図)と同様に、鍵生成部12から暗号鍵 K_1 を供給されることにより、入力される平文Pを暗号文Cに変換し、ICカード2に転送する。

一方ICカード2には、第10図における鍵生成部22の代わりに鍵レジスタ25および反転処理部26が設けられ、鍵レジスタ25には、銀行センタ1において鍵生成部12が生成する暗号鍵 K_1 が蓄積されている。

反転処理部26は、第4図に示される如く、鍵レジスタ25に蓄積済の暗号鍵 K_1 を抽出し、第一段暗号鍵 K_{11} を第十六段復号鍵 K_{16} 、第二段暗号鍵 K_{12} を第十五段復号鍵 K_{15} 、以下同様にして、第十五段暗号鍵 K_{15} を第二段復号鍵 K_{02} 、第十六段暗号鍵 K_{16} を第一段復号鍵 K_{01} に、それぞれ各段の順序を反転して暗号鍵 K_1 から復号鍵 K_1 を生成し、暗号化処理部21に供給する。

暗号化処理部21は、前述(第11図および第12図)の如く、銀行センタ1において暗号化処理部11が供給された暗号鍵 K_1 の各段の順序を反転

19

した復号鍵 K_1 を供給されることにより、暗号化処理部11と同一構成を有し、暗号化処理部11から転送された暗号文Cを平文Pに変換する。

第5図は、第3図における銀行センタ1に反転処理部18およびセレクト19を追加し、またICカード2にセレクト28を追加することにより、銀行センタ1とICカード2との間の双方向暗号通信を可能としたものである。

第5図においては、銀行センタ1のセレクト19および第2図のセレクト28をそれぞれ「A」側に設定することにより、第3図におけると同様に、銀行センタ1の暗号化処理部11が鍵生成部12から暗号鍵 K_1 を供給されて平文Pを暗号文Cに変換してICカード2に転送し、ICカード2の暗号化処理部21が反転処理部26から復号鍵 K_1 を供給されて暗号文Cを平文Pに変換して出力するが、銀行センタ1のセレクト19およびICカード2のセレクト28をそれぞれ「B」側に設定することにより、第3図におけると逆に、ICカード2の暗号化処理部21が鍵レジスタ2

20

5から暗号鍵 K_1 を供給されて平文Pを暗号文Cに変換して銀行センタ1に転送し、銀行センタ1の暗号化処理部11が反転処理部18から復号鍵 K_1 を供給されて暗号文Cを平文Pに変換して出力する。

次に第6図においては、銀行センタ1において、第3図における鍵生成部12の代わりに、乱数発生部16および鍵レジスタ17が設けられており、またICカード2において、第3図における鍵レジスタ25の代わりに鍵レジスタ27が設けられている。

銀行センタ1において、乱数発生部16は、 $48 \times 16 (= 768)$ ビットの乱数を暗号鍵 K_{11} として発生し、鍵レジスタ17は、乱数発生部16が発生した暗号鍵 K_{11} を蓄積し、暗号化処理部11に供給する。

ICカード2において、鍵レジスタ27には、銀行センタ1において鍵レジスタ17が蓄積する暗号鍵 K_{11} が蓄積されている。

銀行センタ1においては、暗号化処理部11が、

21

22

鍵レジスタ17に蓄積済の暗号鍵 K_{22} を供給されることにより、入力される平文Pを暗号文Cに変換し、ICカード2に転送する。

ICカード2においては、反転処理部26が、前述(第3図)と同様に、鍵レジスタ27に蓄積済の暗号鍵 K_{22} を抽出し、それぞれ各段の順序を反転して復号鍵 K_{22} を生成し、暗号化処理部21に供給する。

暗号化処理部21は、前述(第3図)と同様に、反転処理部26から復号鍵 K_{22} を供給されることにより、暗号化処理部11から転送された暗号文Cを、平文Pに変換する。

次に第7図においては、銀行センタ1には第3図における暗号化処理部11および鍵生成部12の他に、セレクト31乃至33と、乱数発生部34と、鍵レジスタ35とが設けられ、またICカード2には第3図における暗号化処理部21、鍵レジスタ25および反転処理部26の他に、セレクト41乃至43および鍵レジスタ44が設けられている。

2 3

また暗号鍵 K_{22} を供給されている暗号化処理部21も、入力されたセッション乱数Rを暗号化し、暗号化処理部11が生成した同一のセッション暗号鍵 K_{22} を生成し、セレクト42を介して鍵レジスタ44に蓄積する。

反転処理部26は、前述(第3図)と同様に、鍵レジスタ44に蓄積されているセッション暗号鍵 K_{22} を抽出し、それぞれ各段の順序を反転してセッション復号鍵 K_{22} を生成し、セレクト43の「B」側に供給する。

かかる状態で、銀行センタ1におけるセレクト31乃至33、およびICカード2におけるセレクト41乃至43を、それぞれ「B」側に切替えると、銀行センタ1においては、暗号化処理部11が、鍵レジスタ35に蓄積されているセッション暗号鍵 K_{22} をセレクト33を介して供給されることにより、該セッションにおいて入力される平文Pを暗号文Cに変換し、セレクト32を介してICカード2に転送する。

ICカード2においては、暗号化処理部21が、

当初、銀行センタ1におけるセレクト31乃至33、およびICカード2におけるセレクト41乃至43は、何れも「A」側に設定されている。

その結果、銀行センタ1においては、鍵生成部12がマスタ鍵 K_{22} から生成した暗号鍵 K_{22} が、セレクト33を介して暗号化処理部11に供給されており、またICカード2においては、鍵レジスタ25に蓄積されている暗号鍵 K_{22} がセレクト43を介して暗号化処理部21に供給されている。

かかる状態で、乱数発生部34は、各セッション毎にそれぞれ $48 \times 16 (= 768)$ ビットから成るセッション乱数Rを発生し、セレクト31を介して暗号化処理部11に入力すると共に、ICカード2にも転送し、セレクト41を介して暗号化処理部11と同一構成を有する暗号化処理部21に入力する。

暗号鍵 K_{22} を供給されている暗号化処理部11は、入力されたセッション乱数Rを暗号化してセッション暗号鍵 K_{22} を生成し、セレクト32を介して鍵レジスタ35に蓄積する。

2 4

反転処理部26からセレクト43を介してセッション復号鍵 K_{22} を供給されることにより、銀行センタ1からセレクト41を介して転送される暗号文Cを平文Pに変換し、セレクト42を介して出力する。

以上により、銀行センタ1とICカード2の間では、各セッション毎に異なるセッション乱数Rから暗号化処理部11と、暗号化処理部21および反転処理部26とにより暗号化されて生成されたセッション暗号鍵 K_{22} およびセッション復号鍵 K_{22} を用いて暗号通信が実行される。

次に、第8図および第9図に基づき本発明の一実施例による認証システムを説明する。

第8図において、銀行センタ1には前述(第13図)と同様に、暗号化処理部11、鍵生成部12、乱数発生部13および比較部14が設けられているが、ICカード2には鍵生成部23の代わりに鍵レジスタ25が設けられている。

鍵レジスタ25には、銀行センタ1において鍵生成部12がオリジナル鍵Kから生成する認証

2 5

2 6

鍵 K_a が蓄積されており、暗号化処理部21の各段に供給されている。

かかる状態で、銀行センタ1に設けられている乱数発生部13は、前述(第13図)と同様に、乱数 R_1 を発生して暗号化処理部11に入力すると共に、ICカード2にも転送し、暗号化処理部21に入力する。

各暗号化処理部11および21は、前述(第13図)と同様に、それぞれ鍵生成部12および鍵レジスタ25から認証鍵 K_a を供給されることにより、入力される乱数 R_1 をそれぞれ暗号化乱数 R_{e1} および R_{e2} に変換し、銀行センタ1に設けられた比較部14に伝達する。

比較部14は、暗号化処理部11から伝達される暗号化乱数 R_{e1} と、暗号化処理部21から伝達される暗号化乱数 R_{e2} とを比較し、両者が一致した場合には、銀行センタ1はICカード2を認証する。

次に第9図において、銀行センタ1には、第8図における鍵生成部12の代わりに、乱数発生部

16および鍵レジスタ17が設けられており、またICカード2には、第8図における鍵レジスタ25の代わりに鍵レジスタ27が設けられている。

銀行センタ1において、乱数発生部16は、 $48 \times 16 (= 768)$ ビットの乱数を認証鍵 K_a として発生し、鍵レジスタ17は、乱数発生部16が発生した認証鍵 K_a を蓄積し、暗号化処理部11に供給する。

ICカード2において、鍵レジスタ27には、銀行センタ1において鍵レジスタ17が蓄積する認証鍵 K_a が蓄積され、暗号化処理部21の各段に供給している。

かかる状態で、銀行センタ1に設けられている乱数発生部13は、前述(第8図)と同様に、乱数 R_1 を発生して暗号化処理部11に入力すると共に、ICカード2にも転送し、暗号化処理部21に入力する。

各暗号化処理部11および21は、前述(第8図)と同様に、それぞれ鍵レジスタ17および27から認証鍵 K_a を供給されることにより、入力

27

される乱数 R_1 をそれぞれ暗号化乱数 R_{e1} および R_{e2} に変換し、銀行センタ1に設けられた比較部14に伝達する。

比較部14は、暗号化処理部11から伝達される暗号化乱数 R_{e1} と、暗号化処理部21から伝達される暗号化乱数 R_{e2} とを比較し、両者が一致した場合には、銀行センタ1はICカード2を認証する。

以上の説明から明らかな如く、本実施例によれば、ICカード2には鍵生成部22を設ける代わりに、銀行センタ1で生成された復号鍵 K_d を蓄積する鍵レジスタ24を設けるか、或いは銀行センタ1で生成された暗号鍵 K_e 、 K_{ee} またはセッション暗号鍵 K_{ss} を蓄積する鍵レジスタ25、27または44と、反転処理部26とを設けることにより、暗号化処理部21が暗号文Cを平文Pに変換することが可能となり、所要の暗号通信が実現可能となり、またICカード2に鍵生成部23を設ける代わりに、銀行センタ1で生成された認証鍵 K_a または K_{aa} を蓄積する鍵レジスタ25ま

28

たは27を設けることにより、暗号化処理部21が乱数 R_1 を暗号化乱数 R_{e2} に変換可能となり、所要の認証が可能となる。

なお、第2図乃至第9図はあく迄本発明の一実施例に過ぎず、例えば第2図における暗号鍵 K_e はオリジナル鍵 K_e から鍵生成部12および鍵生成部15により生成されるものに限定されることは無く、乱数発生部16および反転処理部18により生成する等、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。また第2図、第6図および第7図に示される暗号通信システムは、一方通信のみに限定されることは無く、第3図に対する第5図の如く、双方通信とすることも考慮されるが、かかる場合にも本発明の効果は変わらない。また第8図および第9図に示される認証システムは、銀行センタ1からICカード2を一方認証するものに限定されることは無く、ICカード2から銀行センタ1の認証、更には双方認証とすることも考慮されるが、かかる場合にも本発明の効果は変わらない。更に本

29

30

発明の対象とする装置 100、300 および相手装置 200、400 は、IC カード 2 と銀行センタ 1 とに限定されぬことは言う迄も無い。

(発明の効果)

以上、本発明(請求項 1 乃至請求項 6)によれば、装置には DES 方式に基づく暗号処理に必要な鍵生成部を設ける必要が無く、装置の小形化、軽量化および経済化を大幅に向上する。

4. 図面の簡単な説明

第 1 図は本発明の原理を示す図で、同図(a)は請求項 1 に関する原理を示し、同図(b)は請求項 2 に関する原理を示し、同図(c)は請求項 3 に関する原理を示し、同図(d)は請求項 4 に関する原理を示し、第 2 図は本発明(請求項 1 および請求項 5)の一実施例による暗号通信システムを示す図、第 3 図は本発明(請求項 2 および請求項 5)の一実施例による暗号通信システムを示す図、第 4 図は第 3 図における反転処理部の一

を示す図、第 5 図は第 3 図に対応する双方向暗号通信システムを示す図、第 6 図は本発明(請求項 2 および請求項 6)の一実施例による暗号通信システムを示す図、第 7 図は本発明(請求項 3 および請求項 5)の一実施例による暗号通信システムを示す図、第 8 図は本発明(請求項 4 および請求項 5)の一実施例による認証システムを示す図、第 9 図は本発明(請求項 4 および請求項 6)の一実施例による認証システムを示す図、第 10 図は従来ある暗号通信システムの一例を示す図、第 11 図は第 10 図における銀行センタ側装置の一例を示す図、第 12 図は第 10 図における IC カード側装置の一例を示す図、第 13 図は従来ある認証システムの一例を示す図である。

図において、1 は銀行センタ、2 は IC カード、11 および 21 は暗号化処理部、12、22 および 23 は鍵生成部、13、16 および 34 は乱数発生部、14 は比較部、17、24、25、27、35 および 44 は鍵レジスタ、18 および 26 は反転処理部、19、28、31 乃至 33 および 4

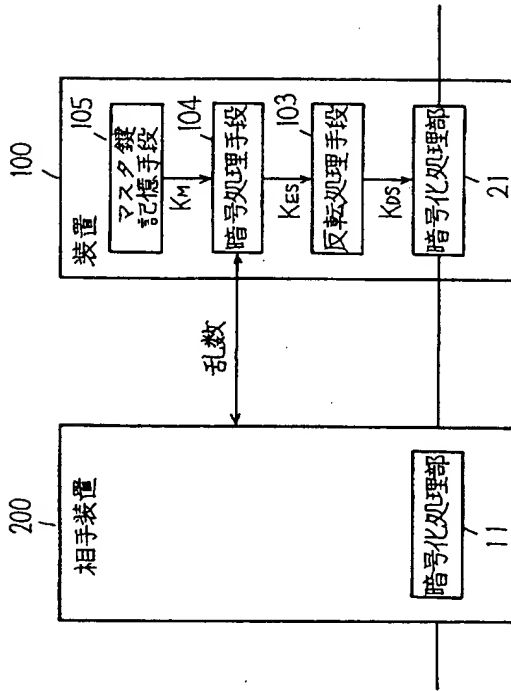
3 1

3 2

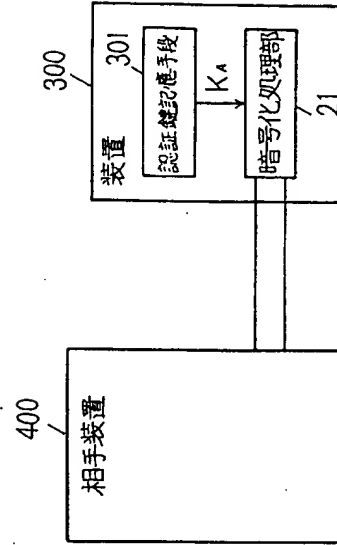
1 乃至 43 はセレクタ、100 および 300 は装置、200 および 400 は相手装置、101 は鍵記憶手段、102 は暗号鍵記憶手段、103 は反転処理手段、104 は暗号処理手段、105 はマスク鍵記憶手段、301 は認証鍵記憶手段、を示す。

代理人 井理士 井 桁 貞 一

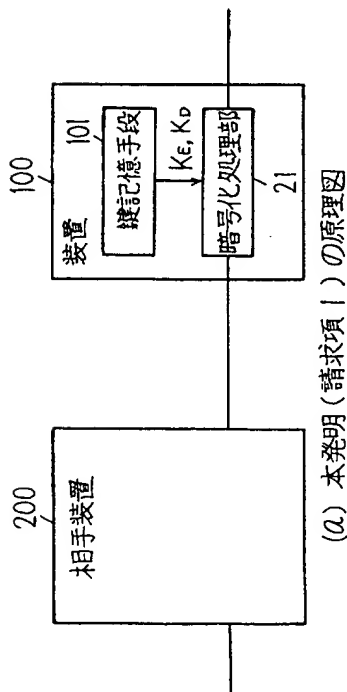




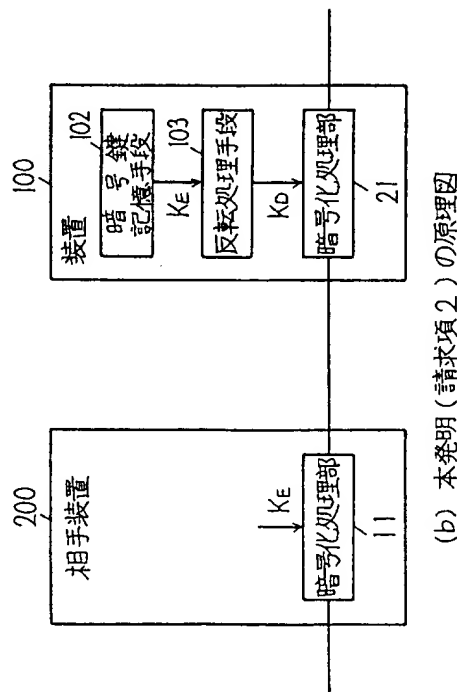
(c) 本発明(請求項3)の原理図



(d) 本発明(請求項4)の原理図



(a) 本発明(請求項1)の原理図

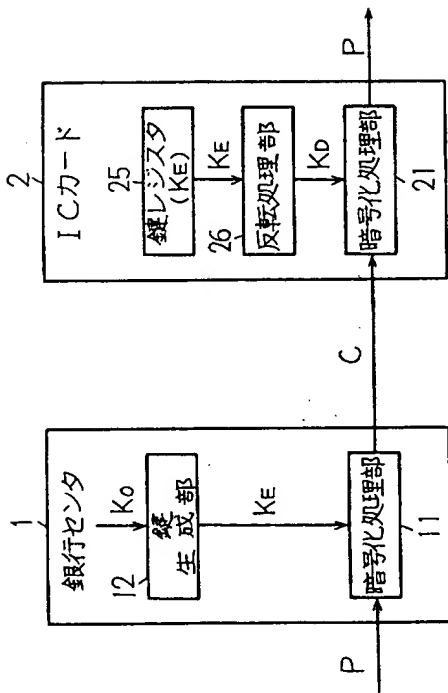


(b) 本発明(請求項2)の原理図

本発明の原理図
第1図(その1)

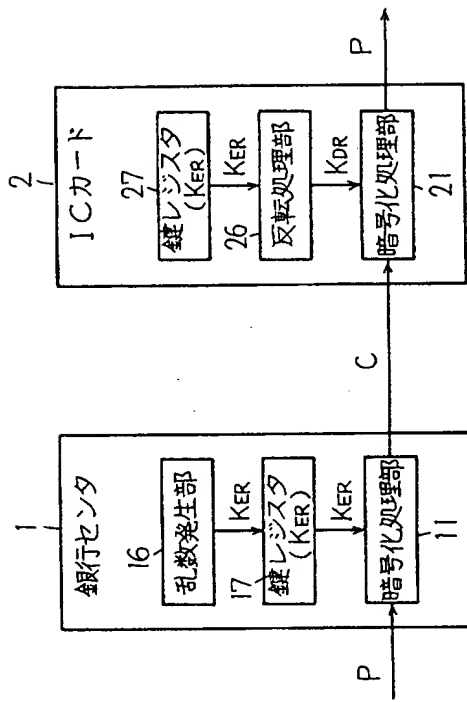
第1図(その2)

本発明の原理図



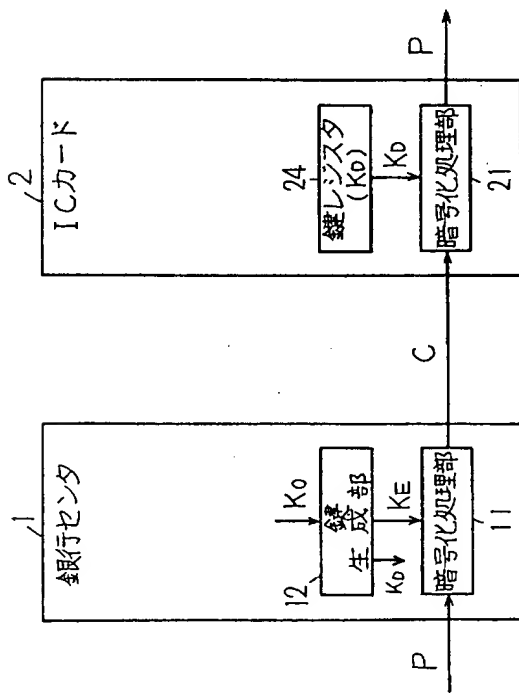
本発明(請求項2および請求項5)による暗号通信システム

第 3 図



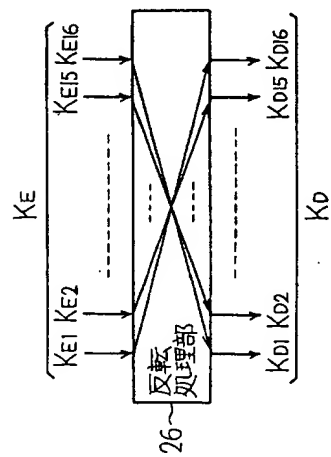
本発明(請求項2および請求項6)による暗号通信システム

第 6 図



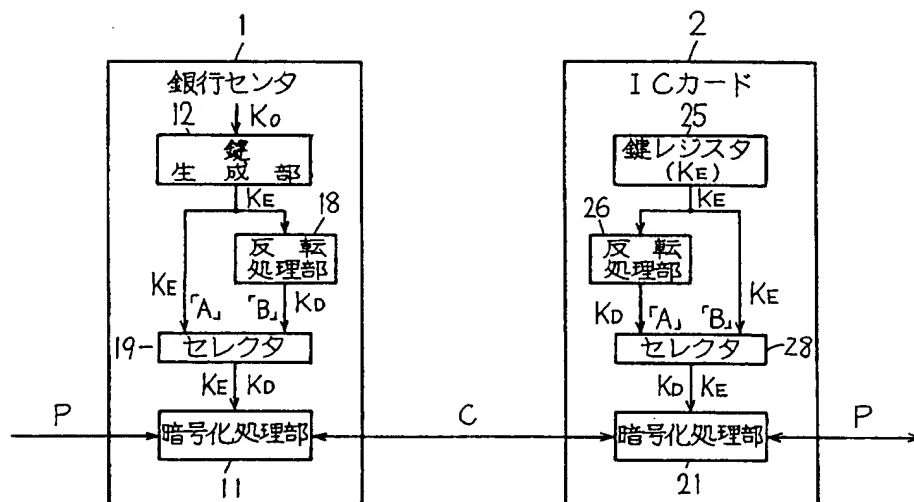
本発明(請求項1および請求項5)による暗号通信システム

第 2 図



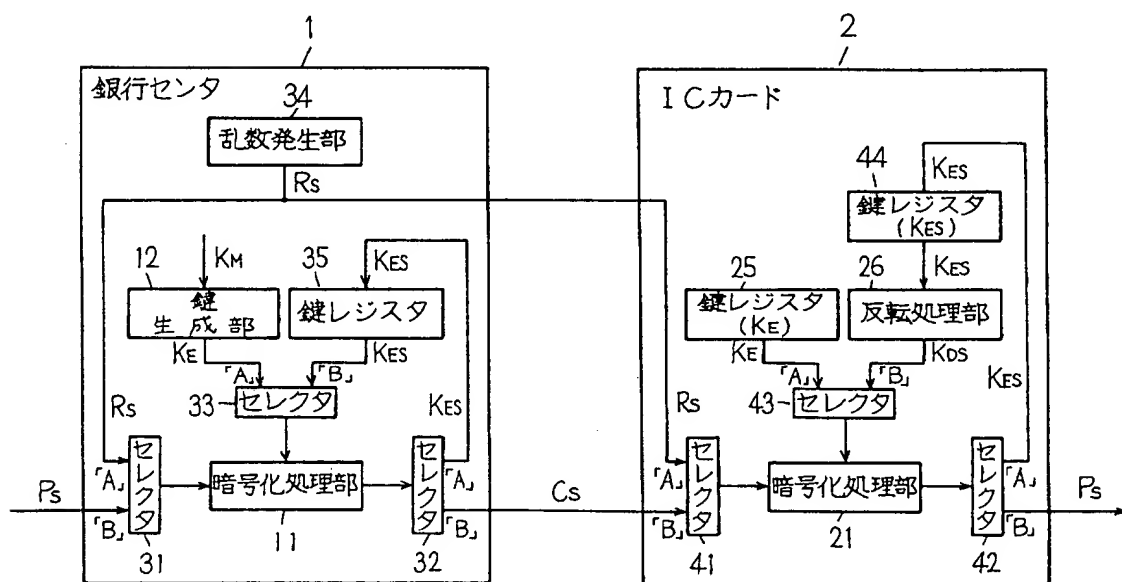
第3図における反転処理部

第 4 図



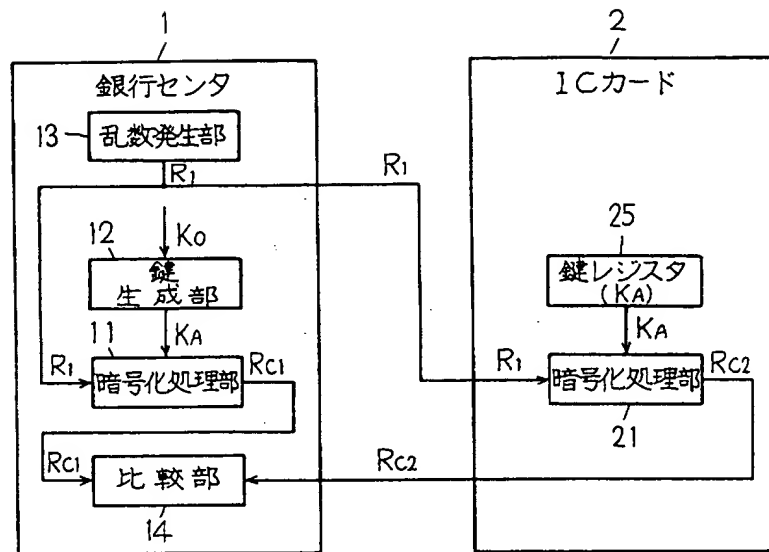
第3図に対応する双方向暗号通信システム

第 5 図



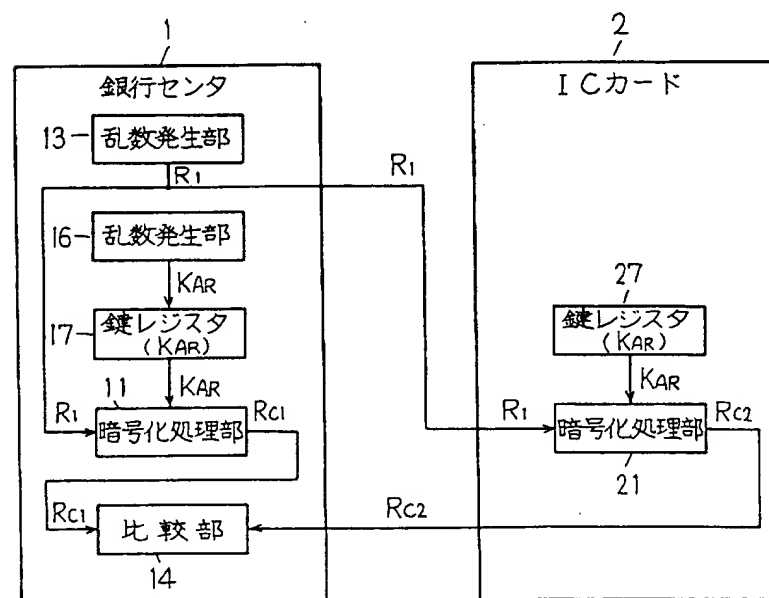
本発明(請求項3および請求項5)による暗号通信システム

第 7 図



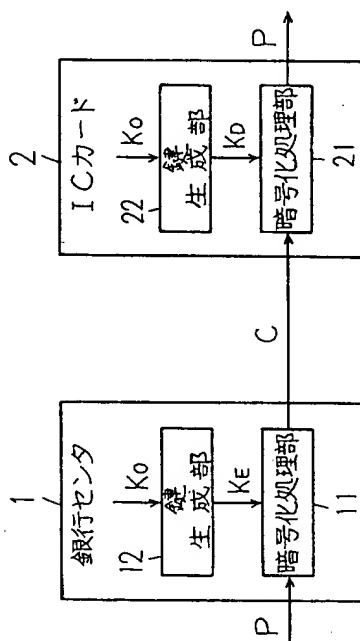
本発明(請求項4および請求項5)による認証システム

第 8 図



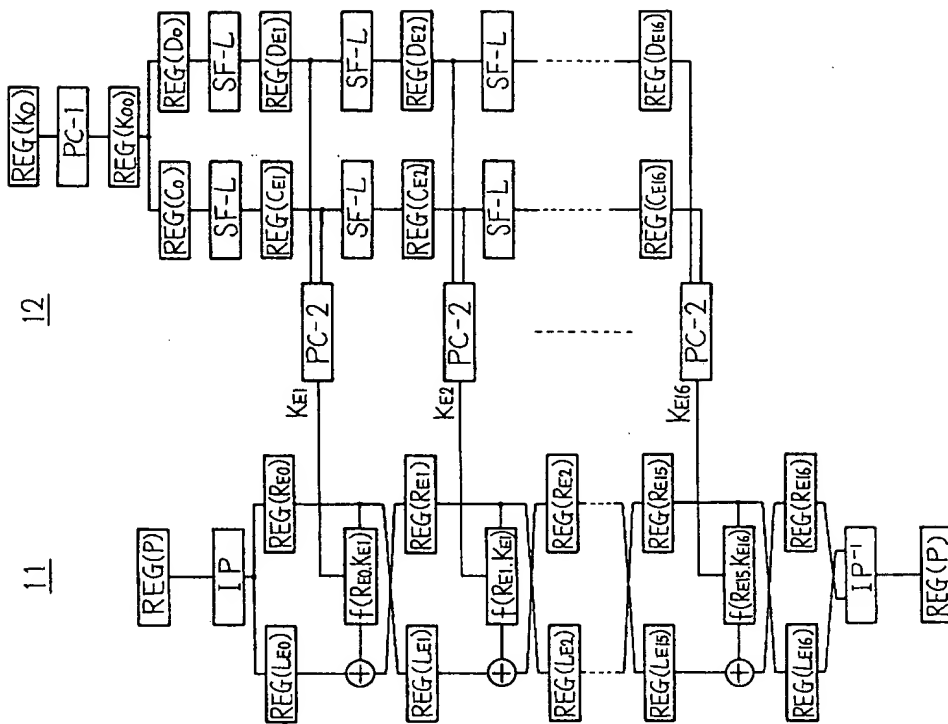
本発明(請求項4および請求項6)による認証システム

第 9 図



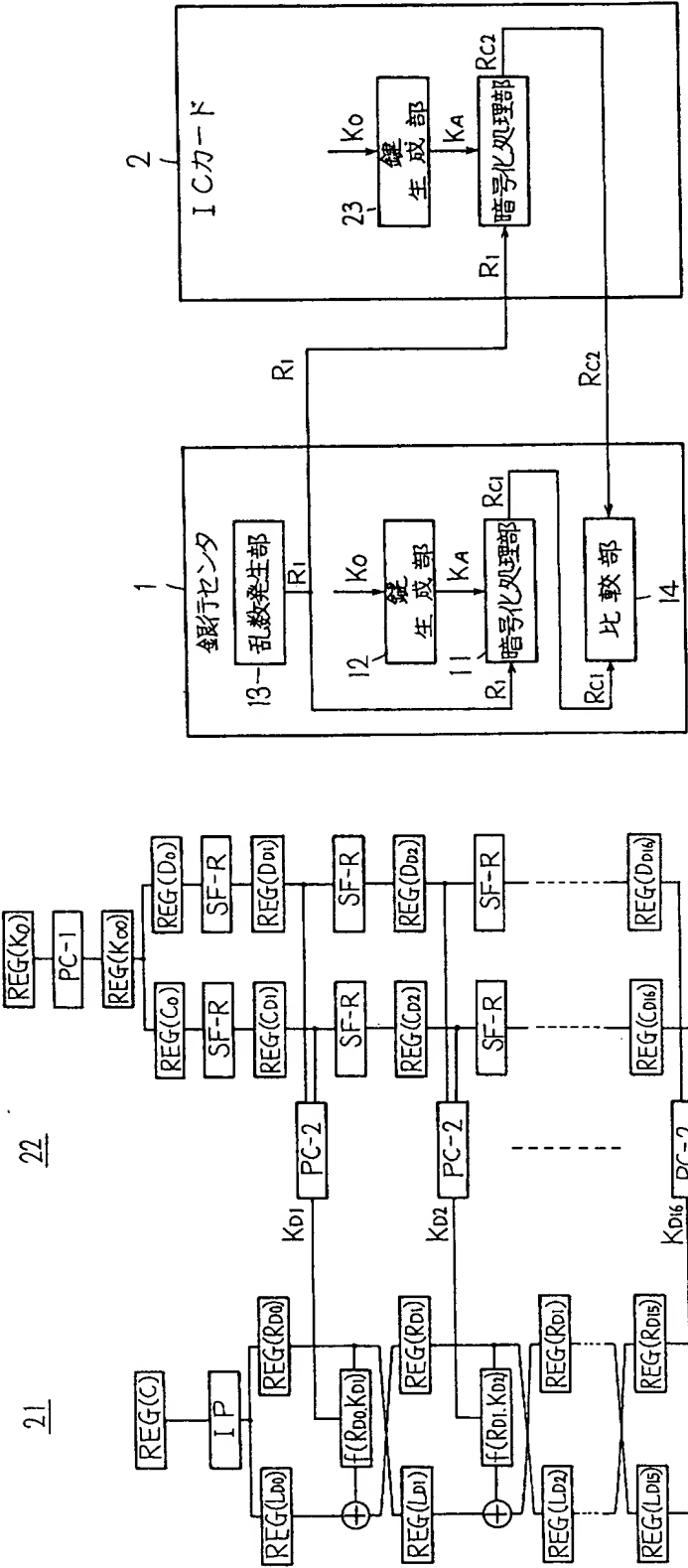
従来ある暗号通信システム

第 10 図

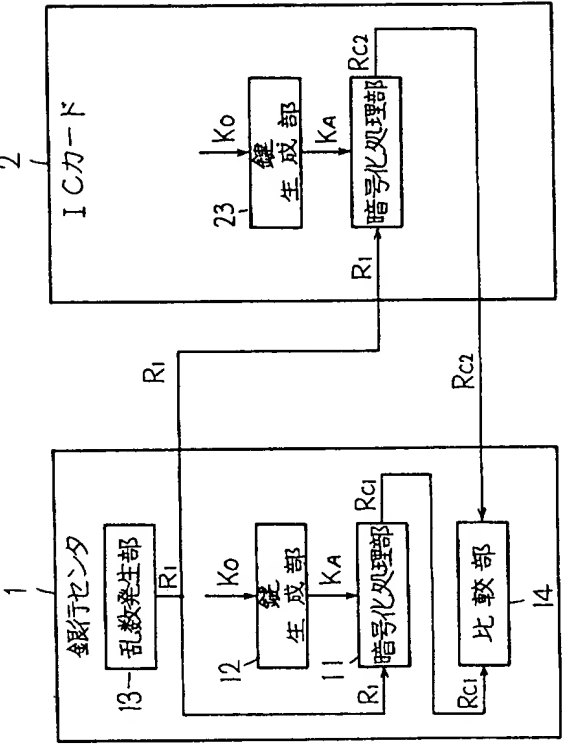


第10図における銀行センタ側装置

第 11 図



第10図におけるICカード側装置
第 12 図



従来ある認証システム
第 13 図